What is claimed is:

1. A method of detecting the falsification of contents of a plurality of files stored on a computer medium, comprising:

producing first falsification-detecting information corresponding to current filenames or current contents of the plurality of files; and

detecting the falsification of the contents of the plurality of files by comparing second falsification-detecting information corresponding to the filenames or contents of the plurality of files at the time of registration or renewal with the first falsification-detecting information.

2. The method of claim 1 wherein said first falsification-detecting information comprises a hash value.

3. A detector for detecting the falsification of contents of a plurality of files stored on a computer, comprising:

a falsification-detecting-information producing/processing unit to produce first falsification-detecting information corresponding to current filenames or current contents of the plurality of files; and

a falsification-detection processing unit to compare second falsification-detecting information corresponding to the filenames or contents of the plurality of files at the time of their registration or renewal and the first falsification-detecting information, thereby detecting any falsification in the contents.

4. The detector of claim 3 wherein said first falsification-detecting information comprises a hash value.

5. A system for detecting the falsification of contents of a plurality of files stored on a computer, comprising:

a falsification production means for producing first falsification-detecting information corresponding to current filenames or current contents of the plurality of files; and

a falsification-detection means for comparing second falsification-detecting information corresponding to the filenames or contents of the plurality of files

at the time of their registration or renewal with the first falsification-detecting information, thereby detecting any falsification in the contents.

6. A method using a computer for checking the validity of a plurality of related files, comprising:

producing a first cumulative hash value at a first time comprising a plurality of first hash values, wherein a first hash value of the plurality of first hash values is associated with a related file of said plurality of related files; and

comparing said first cumulative hash value with a second cumulative hash value produced at a second time, said second cumulative hash value comprising a plurality of second hash values, wherein a second hash value of the plurality of second hash values is associated with the related file of said plurality of related files.

7. The method of claim 6 wherein said first hash value comprises hashing a contents of the related file.

8. The method of claim 6 wherein said first hash value comprises hashing a filename, comprising a path name, of the related file.

9. The method of claim 6 wherein the plurality of related files correspond to a plurality of Web pages.

10. The method of claim 6 wherein the first cumulative hash value is a concatenation of the plurality of first hash values.

11. The method of claim 6 wherein the first cumulative hash value is a hash of a concatenation of the plurality of first hash values.

12. A system for checking the validity of a plurality of related files, comprising:

a falsification producing module for producing a first cumulative hash value at a first time comprising a plurality of first hash values, wherein a first hash value of the plurality of first hash values is associated with a related file of said plurality of related files; and

a falsification detection module for comparing said first cumulative hash value with a second cumulative hash value produced at a second time, said second

cumulative hash value comprising a plurality of second hash values, wherein a second hash value of the plurality of second hash values is associated with the related file of said plurality of related files.

13. A system for checking the validity of a plurality of related files, comprising:

a means for producing a first cumulative hash value at a first time comprising a plurality of first hash values, wherein a first hash value of the plurality of first hash values is associated with a related file of said plurality of related files; and

a means for comparing said first cumulative hash value with a second cumulative hash value produced at a second time, said second cumulative hash value comprising a plurality of second hash values, wherein a second hash value of the plurality of second hash values is associated with the related file of said plurality of related files.

14. A method for embedding security information in a plurality of files, wherein said plurality of files are related, said method comprising:

determining a first set comprising a first plurality of first cryptographic values, wherein a first cryptographic value of said first set is generated using first information including contents of a file of said plurality of files;

determining a hashed first set by hashing said plurality of first cryptographic values in said first set; and

generating an internet mark comprising said hashed first set, said internet mark associated with at least one file of said plurality of files.

15. The method of claim 14 wherein said plurality of files are organized hierarchically.

16. The method of claim 15 wherein at least one file of said plurality of files is an HTML file.

17. The method of claim 14 wherein said internet mark is selected from a group consisting of an image, a moving picture, or an audio file.

18. The method of claim 17 wherein said image comprises a visual mark.

19. The method of claim 14 further comprising:

determining a second set comprising a second plurality of second cryptographic values, wherein a second cryptographic value of said second set is generated using second information including a filename of said file of said plurality of files; and

wherein generating said internet mark further comprises said second set.

20. The method of claim 19 wherein said determining said second set uses a sorted list of filenames.

21. A system for embedding security information in a plurality of files, wherein said plurality of files are related, said system comprising:

a falsification-detecting producing module for producing a hashed first set by hashing a plurality of first cryptographic values in a first set, wherein a first cryptographic value of said first set is generated using first information including a contents of a file of said plurality of files; and

an Internet Mark producing module for producing an Internet Mark associated with at least one file of said plurality of files, wherein said hashed first set is embedded in said Internet Mark.

22. The system of claim 21 wherein:

said falsification-detecting producing module further determines a second set comprising a second plurality of second cryptographic values, wherein a second cryptographic value of said second set is generated using second information including a filename of said file of said plurality of files; and

said Internet Mark producing module further embeds said second set in said Internet Mark.

23. A system for embedding security information in a plurality of files, wherein said plurality of files are related, said system comprising:

means for determining a first set comprising a first plurality of first cryptographic values, wherein a first cryptographic value of said first set is generated using first information including a contents of a file of said plurality of files;

means for determining a hashed first set by hashing said plurality of first cryptographic values in said first set;

means for determining a second set comprising a second plurality of second cryptographic values, wherein a second cryptographic value of said second set is generated using second information including a filename of said file of said plurality of files; and

means for generating a digital watermark using said hashed first set, said second set and an internet mark, said internet mark associated with at least one file of said plurality of files.

24. A method for detecting tampering in at least one file of a plurality of files associated with a home page, wherein each file of said plurality of files has a corresponding filename and file contents, said method comprising:

generating a first hash value for each filename, wherein each filename includes a corresponding directory path;

forming at a current time a current filename hash value by concatenating first hash values;

generating a second hash value for each file contents; and

forming at said current time a current contents hash value by hashing a result, said result generated by concatenating second hash values.

25. The method of claim 24 further comprising:

determining tampering of any filenames of said plurality of files at said current time by comparing said current filename hash value with a previous filename hash value, said previous filename hash value generated at said previous time.

26. The method of claim 25 further comprising:

when said determining tampering of any filenames indicates no tampering of filenames, determining tampering of any contents of said plurality of files at said current time by comparing said current contents hash value with a previous contents hash value, said previous contents hash value generated at a previous time.

27. The method of claim 24 wherein said concatenating first hash values is performed after said first hash values are sorted.

28. An intermediary device for determining a location of a falsification of contents of a document, wherein said document is sent from a server to a client through said intermediary device in response to a request by said client, and wherein said document includes an Internet Mark (IM) with embedded falsification information, said intermediary device comprising:

a falsification detection module for detecting by using said IM, if said contents has been falsified; and

a notification module for notifying said server and said client of said location when said falsification detection module indicates said contents has been falsified, wherein said location includes a route between said server and said intermediary device.

29. The intermediary device of claim 28 further comprising an Internet Mark checking module for determining if said Internet Mark was removed from said document.

30. The intermediary device of claim 28, wherein said falsification information includes a hash value.

31. A client system for determining a location of a falsification of contents of a document, wherein said document is sent from a server to an exit gate to said client system responsive to a client system request, and wherein said contents includes an Internet Mark (IM) with embedded falsification information, said client system comprising:

a falsification detection module for detecting by using said IM, if said contents has been falsified; and

a display for displaying said location when said falsification detection module indicates said contents has been falsified, wherein said location includes a route between said exit gate and said client.

32. The client system of claim 31 further comprising an Internet Mark checking module for determining if said Internet Mark was removed from said document.

33. A method for determining a location of falsification of contents of a document sent from a server to a client over a communications path, said

communications path comprising a first path from said server to an intermediate computer and a second path from said intermediate computer to said client, wherein said contents comprises an Internet Mark with embedded cryptographic information, said method comprising:

sending said document by said server to said intermediate computer over said first path, when said server validates said contents using said embedded cryptographic information;

determining said location comprises said first path, if said intermediate computer detects said contents has been falsified;

sending said document by said intermediate computer to said client over said second path, when said intermediate computer validates said contents using said embedded cryptographic information; and

determining said location comprises said second path, if said client detects said contents has been falsified.

34. The method of claim 33 wherein said document is a HTML document.

35. A system for determining a location of falsification of contents of a file sent over a communications path, wherein said contents comprises an Internet Mark with embedded cryptographic information, and wherein said communications path comprises a first path coupled with a second path, said system comprising:

a server for sending said file over said first path, when said server validates said contents using said embedded cryptographic information;

an intermediate computer coupled with said server using said first path, said intermediate computer for determining said location comprises said first path, if said intermediate computer detects said contents has been falsified, and for sending said file over said second path, when said intermediate computer validates said contents using said embedded cryptographic information; and

a client coupled with said intermediate computer using said second path, said client for determining said location comprises said second path, if said client detects said contents has been falsified.